Program Research Project

DOD INFORMATION SHARING WITH DOMESTIC EMERGENCY PARTNERS FOR DSCA MISSIONS

BY

COLONEL ROBERT A. HEDGEPETH
United States Army

DISTRIBUTION STATEMENT A:
Approved for Public Release.
Distribution is Unlimited.

USAWC CLASS OF 2011

This PRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College, Carlisle Barracks, PA 17013-5050

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 06-06-2011	**2. REPORT TYPE** Program Research Project	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE

Atoms DOD Information Sharing with Domestic Emergency Partners for DSCA Missions

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

COL Robert A. Hedgepeth

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

CAPT (Ret) David Willmann
Department of Distance Education

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Large scale terrorist acts and natural disasters in the last ten years have prompted aid responses from many different federal, state, and local government agencies as well as non-government and private volunteer organizations and corporations. Each responding entity needs information to carry out its support functions and, in turn, will have information to share with other entities involved in the incident. U.S. military organizations providing support must proactively identify and implement ways to collaborate and share information with other domestic emergency response partners, including the public, while protecting and defending military networks.

In order to do this prior to an incident, common points of coordination must be defined and the terms and conditions for establishing data sharing relationships must be established. This must occur with the entities most likely to respond to large-scale incidents. Policies for forming ad-hoc relationships must be developed and communicated so other entities can prepare to participate more collaboratively.

Strengthening relationships in this manner will promote an informed response at critical times when lives hang in the balance.

15. SUBJECT TERMS

Defense Support Civilian Authorities Communications Social Media

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UNCLASSIFED	**b. ABSTRACT** UNCLASSIFED	**c. THIS PAGE** UNCLASSIFED	UNLIMITED	34	**19b. TELEPHONE NUMBER** *(include area code)*

USAWC PROGRAM RESEARCH PROJECT

DOD INFORMATION SHARING WITH DOMESTIC EMERGENCY PARTNERS FOR DSCA MISSIONS

by

Colonel Robert A. Hedgepeth
United States Army

Topic Approved By

Captain David W. Willmann
United States Navy Retired
Faculty Instructor

This PRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR:	COL Robert A. Hedgepeth
TITLE:	DOD Information Sharing with Domestic Emergency Partners for DSCA Missions
FORMAT:	Program Research Project
DATE:	6 June 2011 WORD COUNT: 5,691 PAGES: 34
KEY TERMS:	Defense Support Civilian Authorities Communications Social Media
CLASSIFICATION:	Unclassified

Large scale terrorist acts and natural disasters in the last ten years have prompted aid responses from many different federal, state, and local government agencies as well as non-government and private volunteer organizations and corporations. Each responding entity needs information to carry out its support functions and, in turn, will have information to share with other entities involved in the incident. U.S. military organizations providing support must proactively identify and implement ways to collaborate and share information with other domestic emergency response partners, including the public, while protecting and defending military networks.

In order to do this prior to an incident, common points of coordination must be defined and the terms and conditions for establishing data sharing relationships must be established. This must occur with the entities most likely to respond to large-scale incidents. Policies for forming ad-hoc relationships must be developed and communicated so other entities can prepare to participate more collaboratively.

Strengthening relationships in this manner will promote an informed response at critical times when lives hang in the balance.

DOD INFORMATION SHARING WITH DOMESTIC EMERGENCY PARTNERS FOR DSCA MISSIONS

Pre-established relationships and mechanisms for information sharing must be established prior to disasters and periodically reviewed and maintained for use during DOD homeland defense and disaster relief missions to assure a fully coordinated response by facilitating the exchange of appropriate information in a timely manner with DOD partner organizations. At all levels, the DOD must proactively establish and maintain these relationships in order to enhance informed decision making and performance of domestic operations.

Background

The Department of Defense (DOD) provides support to civilian authorities after natural disasters and when the security of the U.S. requires augmentation by the military forces in order to save life and limb and to protect critical infrastructure.[1] In all cases, and in accordance with the U.S. Constitution, the military assistance provided is in support of civil authorities.[2]

This support is provided to civilian authorities in accordance with Homeland Security Presidential Directive 5[3] which establishes the Department of Homeland Security's (DHS) National Incident Management System (NIMS). NIMS is a key part of the National Response Framework and "[e]stablishes a systematic approach for managing incidents nationwide."[4] It is coordinated with the National Strategy for Homeland Security and Response Partner Guides. These guides define "key roles and actions for local, tribal,[5] State, federal, and private-sector response partners."[6]

Support is provided in a scalable manner, although rules governing assistance requests vary from state to state. Small responses usually involve requests elevated from county (or equivalent) emergency management coordinators to an agency representing the state's governor. The governor may then provide National Guard assistance to work alongside other agencies who are either responding at the direction of the governor or via separate mutual aid agreements.[7] National Guard assistance is usually performed in State Active Duty status, funded directly by that state's government, or federally funded in Title 32 status.[8] If the incident is declared a federal disaster, the federal government will reimburse at least a portion of state funds expended for this purpose.[9]

A typical National Guard response might include command and control, aviation, engineer, medical, communications, transportation, and logistics support as well as trained and disciplined manpower for security and presence patrols. These missions exemplify the concept of 'dual-use;' the application of the military's war-fighting training and equipment for a military domestic response.[10]

If the scope of the disaster surpasses a state's ability to respond in this manner, Emergency Management Assistance Compact (EMAC) agreements may be executed to provide interstate mutual aid of civilian and military capabilities. The agreements define the terms and conditions of support, liability, and fund reimbursement.[11]

An even larger disaster, one that exceeds the capacity of local and regional assets or requires special capabilities, may involve a federal response. This response is typically made under the provisions of the Stafford Act,[12] which allows the President to direct the use of DOD resources to perform emergency work "which is essential for the preservation of life and property."[13] At this point, United States Northern Command

(NORTHCOM) will involve active duty and reserve forces in a Title 10 status, provided in a supporting role to civilian authorities as well.[14]

Examples of Defense Support to Civilian Authorities (DSCA)[15] missions for relief following natural disasters range from requests for National Guard assistance at the local, county, tribal and state levels for tornados, winter storms, and floods to full scale, Title 10 and 32 responses for catastrophic events. Hurricane Katrina, which dramatically impacted the Gulf Coast in 2005, is an example of such a catastrophic event. The state and federal response to Katrina included approximately 72,000 military personnel,[16] and was the largest DSCA response in U.S. history.[17]

Responses requiring personnel and equipment in numbers comparable to the Katrina response could also be required in homeland defense situations. These events involve a manmade or natural threat or attack to the United States, such as those occurring in the aftermath of the September 11, 2001 terrorist attacks or a large, widespread Chemical, Biological, Radiological or Nuclear (CBRN) incident.[18] Together, homeland defense, natural disasters, and other “equivalent emergencies that endanger life and property or disrupt the usual process of government” are termed domestic emergencies.[19]

In all cases, disaster response is comprised of activities by numerous government, corporate, charitable, and private organizations at all levels.

> “Citizens are not well served if disaster response is not based on the joint, interagency, inter-governmental and multi-national (JIIM) partnership….It is wasteful and counterproductive not to engage early and regularly with civilian and military partners who, acting synchronously, provide valuable mutual assistance to one another.”[20]

Information Sharing

One large part of ‘acting synchronously’ during domestic emergencies is the exchange of electronic information between the many entities responding to the event. Vice Chairman of the Joint Chiefs of Staff, General James Cartwright, in speaking of the military’s capabilities to share information with partner agencies, reinforced the similarities between current offensive operations in Afghanistan and Iraq and DSCA missions. In theater “…we fight interagency and coalition,”[21] he said, emphasizing the close relationships between U.S. military forces and other partners. Similar relationships hold true for DSCA missions.[22]

Flexible, open communication systems and widespread sharing of information is contrary to most actions required to ensure the integrity and security of information systems. DOD goes to great efforts to protect and defend its networks and data from intrusion, attack, and tampering. Policies exist to govern accessing, reception, sharing and transmitting files within and outside the DOD network domain. DOD elements must proactively engage with partner agencies to define the terms and conditions under which information sharing will occur so that these details and technologies will not have to be negotiated in the midst of a domestic emergency.

Much of the criticism related to the federal response to Hurricane Katrina related to “significant organization and coordination problems” and lapses in communications and situational awareness.[23] Failure to plan and conduct proper coordination for future events will continue to contribute to unacceptable delays and deny critical planning information from those charged with making decisions and saving lives.

This coordination may include guidelines for permissible file formats, hardware and software security settings, definitions of document designations, and instructions for handling and disclosing information to others. Some commonly encountered types of information requiring designations include: controlled unclassified information (CUI)[24] such as sensitive information, [25] operational and tactical information, and Law Enforcement Sensitive (LES) information; personally identifiable information (PII); Protected Critical Infrastructure Information (PCII),[26] and information that may be subject to protection under the Health Insurance Portability and Accountability Act (HIPAA).[27] This coordination should also cover the designation and handling of information labeled 'For Official Use Only (FOUO)' under the requirements of the Freedom of Information Act (FOIA).[28]

Delineating exactly how these information exchanges take place during DSCA response situations demand a basic mission analysis: **who, what, why, when, where, and how,** by domestic operations planners in conjunction with points of contact at partner agencies.[29] Once these questions are resolved for mission planners, then a framework for coordination can be established and executed to ensure timely and secure information flow with domestic emergency partners during DSCA missions.

- Who are likely partners that need or have relevant information?
- What types of critical information are expected to be shared with others?
- Why is the information necessary?
- When will the information be needed?
- Where will the information be needed?

- How will the information be coordinated, transmitted, received and used, and how will the integrity of the information be maintained?

Who. Who are likely partners that need or have relevant information? Information may be sent and received by military forces supporting civilian authorities during domestic emergencies, to and from many different and varied entities outside the DOD network domain.[30] These entities may include other government organizations (OGO), foreign government or military organizations, non-governmental organizations (NGO), private volunteer organizations (PVO), corporate partners, and the public.

Some of these potential partners may seem unlikely to traditional emergency response planners. One usually associates the U.S. military with helping other countries during natural disasters, not the reciprocal. In the aftermath of Hurricane Katrina; however, the U.S. did receive assistance from the governments and militaries of Mexico[31] and Canada.[32] Canada has provided assistance to the U.S. before, and a Strategic Operations Information Sharing Plan of Action exists between the two nations.[33] This event; however, set a precedent for Mexican assistance and reinforces the requirement for multi-national cooperation.

Another group of seemingly unlikely disaster relief partners include corporations. Walmart is the world's number one retailer, with over 2.1 million employees and over 8,300 stores.[34] According to Brian Koon, Director of Emergency Management for Walmart, the corporation set a new precedent for private sector emergency management during the aftermath of Hurricane Katrina. Katrina damaged over 120 Walmart stores, but they mobilized their corporate logistics system to quickly set up temporary stores in parking lots of their damaged or destroyed properties. They assembled nearly 2,500 truckloads of merchandise to be sold or donated for survival and recovery efforts.[35]

Walmart realized through this effort that better coordination with other entities and officials would enable a larger percentage of the post-disaster population to be served better. An example of wasted resources cited by Koon relates a water distribution point set up by emergency management facilities in the same parking lot as a temporary store, which also had supplies of water. Meanwhile, there were other areas in the same county that were more than ten miles away from any water distribution points. The point Koon makes is that Walmart and emergency management officials should share data about where they were distributing supplies so that the duplication of effort could be reduced and underserved areas better accommodated.[36]

Townsend and Moss, in their analysis of telecommunications in disasters, quote researchers of Japan's 1996 Kobe earthquake:

> "The basic lesson from Kobe is that the usual approach of disaster communications, traditionally based on military-style public safety agencies that are operating in a topdown manner and share information with "civilians" only on a "need-to-know" basis, should be replaced. Instead, we should set up an open-access emergency system - open to inputs from a wide variety of public and private participants and with open to access to that information."[37]

While the Kobe article focuses specifically on voice telecommunications, Townsend and Moss' research also analyzed telecommunications systems and their uses during other significant events. They examined the 2004 Indian Ocean Tsunami, the September 11, 2001 terrorist attacks on the World Trade Center, and the 1999 NATO bombing of Belgrade.[38] During this time, the use of cellular telecommunications for voice and data services expanded greatly. They found that:

> "Three decades of social science research in disaster recovery has produced a compelling body of evidence on the important response role of private firms, NGOs, and social networks.[39] International aid agencies are increasingly orienting disaster preparedness and prevention strategies around these institutions.[40] Particularly in very large or prolonged disasters that exhaust official capabilities, NGOs and citizen volunteers are crucial."[41]

The mention of social networks in this 2005 effort is very interesting. As technologies continue to develop, social networking is playing an even larger role in emergency management. Social networking and interested volunteer communities around the world played a very important role during the 2010 earthquake in Haiti, and the 2011 earthquake in Christchurch, New Zealand.[42]

Many different entities have the capabilities and will to assist during domestic emergencies. It is difficult to anticipate which partners will respond to an emergency, regardless of the size of the event. As the next section shows, common points of coordination must be determined to make those initial meetings smoother.

What *and* ***Why****.* What types of critical information are expected to be shared with others and why is the information necessary? Electronic information types likely to be shared during domestic response events might typically include common word processing, spreadsheet, presentation files, graphics, and geo-tagged[43] information used to create common operating pictures.

Any accurate or verifiable information that will aid responders, decision makers, or their operations and logistics planners better serve those affected by a catastrophe falls into this realm. This may include orders, situation update reports, logistics requirements, pictures, videos, briefings, and rosters of personnel, equipment and supplies. Important information may be accessed though: email text and attached data files; files made available on web-based file sharing portals; partner incident management systems; partner mapping solutions, and social media information from websites such as Facebook and Twitter.

Basic email and email with file attachments are the simplest exchanges of information, but they are not without complications which should be solved prior to a domestic emergency. Some networks require messages, or attachments originating from those networks, to be encrypted. This may render the messages unusable by recipients off the domain. Other networks, including the military, block certain types of attachments, such as compressed files commonly known as zip files. Files of this type have the potential to mask viruses which would otherwise escape detection until set forth to damage network or corrupt data. Simply knowing that a system will not accept these types of files is valuable; helping other users understand alternate methods of transmission are required.

RECOMMENDATION: Points of coordination between agencies should include an understanding of the basic capabilities these partners will employ to ensure compatibility for viewing and editing, knowledge of bandwidth limitations, limitations on file sizes user mailboxes are permitted to send or receive, and directories of user names, positions or responsibilities, email addresses and phone numbers for use during the emergency event. Maintaining email and phone directories with frequent updates is also important; especially as personnel change duties. Organizations may have to shift responsibilities based on who is actually available to participate in a disaster response. This is especially true for responders located close to the event, as some people may be personally affected by the disaster and unavailable to perform their normal response duties.

Web-based file sharing portals, such as Microsoft SharePoint,[44] allow users to seek out information posted in a pre-arranged location, instead of relying on the originator to send out the information attached to an email. SharePoint allows tiered access ranging from unrestricted public access, to password protected internet users, to restrictions allowing only intranet or domain user access. Access to SharePoint websites requires prior coordination to ensure security protocols and web browser settings are compatible. Even more training is required for SharePoint users to understand where and how information is stored, and what privileges they have on the site related to reading, modifying, posting and sharing documents. Users may also receive email notifications when new or updated documents are posted.

Incident management systems typically include web-based tools to: log incident information; track requests for materials, assistance and information; and provide electronic chat services and chat logs for incident managers. The systems may include useful information such as mission tracking numbers, locations, point of contact information, and specific mission requirements and approvals. Access to this data is vital for military agencies partnering with emergency managers in order to achieve situational awareness and common incident understanding.

ESI's WebEOC[45] and E Team's NC4[46] are examples of commercially available incident management systems in use by many federal, state and local agencies as well as private corporations. Access to incident management systems is typically password protected and may require training on specific features or agency standard operating procedures. Some of the information contained in these incident management systems can be displayed graphically, or exported to other mapping systems to allow users to quickly ascertain the status of information linked to particular locations.

Although not intended to be utilized for incident management, the National Guard Bureau uses the Joint Information Exchange Environment (JIEE) to maintain situational awareness for tracking alerts, missions, and assets around the country. JIEE facilitates requests for information and assistance among state National Guards and National Guard Bureau and provides visibility of these activities to NORTHCOM.[47]

Geospatial information related to an event or the area around an incident site that can be shared among different partner agencies is referred to as a Common Operating Picture. It is not ‘common’ in the sense that each user sees the same picture. It is, however, common in that each user determines the most important information to meet their needs, based on manipulation of layers containing identical data. Other information can then be hidden so as not to obscure or clutter their map. The Federal Emergency Management Agency’s (FEMA) National Emergency Communications Plan (NECP) defines Common Operating Picture (COP) as:

> “offer[ing] a standard overview of an incident, thereby providing incident information that enables [all involved] to make effective, consistent, and timely decisions. Compiling data from multiple sources and disseminating the collaborative information COP ensures that all responding entities have the same understanding and awareness of incident status and information when conducting operations.”[48]

Common Operating Pictures are frequently found on today’s digitized battlefield with military systems such as Blue Force Tracker, Maneuver Control System, and Movement Tracking System. These systems depict locations of units, equipment and supplies on maps or satellite overlays. The concept of COP is also gaining popularity in emergency management. COP information is displayed graphically, and organized into layers by subject. Just as layers of acetate and symbols can be placed over conventional paper maps to display items of interest, electronic mapping layers can be turned on or off to show different information over background maps or imagery.

The COP information and the resulting layers are managed with mapping software such as ESRI's ArcGIS,[49] favored by GIS professionals, and Google Earth,[50] which is readily available and free. WebEOC and JIEE both offer the option to represent information contained in their incident management systems geospatially. Users can import and export information points or layers in standard file formats common to GIS mapping systems.[51] Points of coordination related to these data exchanges include formats, methods and locations where layer files will be exchanged, and intervals that data will be updated to ensure that the latency, or delay from real time, is known to all parties.

The development and use of Common Operating Pictures took on an entirely new face during Haiti's earthquake in January 2010. This devastating 7.0 magnitude quake killed more than 230,000 people.[52] Nelson and Sigal wrote:

> "The relief efforts became a living laboratory for new applications such as SMS (short message service) texting, interactive on-line maps, and radio-cell phone hybrids. These tools were applied to urgent tasks such as guiding search-and-rescue teams, locating missing persons, and delivering food and water to the populations that needed them the most."[53]

Shortly after the disaster, the Haitian cellular telephone network began to come back on line, and basic text messaging (Short Message Service or SMS) services were re-established. Humanitarian organizations worked to institute as SMS short code[54] that enabled cell phone users to communicate with aid workers. "Reports about trapped persons, medical emergencies and specific needs such as food, water and shelter were received and geo-tagged on maps updated in real time by an international group of volunteers."[55] Within days, thousands of messages were coming through the system."[56]

Creole speakers from around the world volunteered to translate the text messages and provide them back to rescue workers. Another group of volunteers at Tufts University in Boston began using the crisis mapping program Ushahidi,[57] originally developed to map political violence in Kenya, to publish locations where people were trapped and to depict where aid was available. A third volunteer group from the Georgia Institute of Technology converted Ushahidi data to KML for use with Google Earth. This allowed responders with bandwidth restrictions, in this case the U.S. Marines, to better receive the data.[58]

The Ushahidi platform was used for similar purposes after a 6.3 magnitude earthquake struck Christchurch, New Zealand in February 2011. It allowed users to track the availability of medical and humanitarian aid, government notices, building inspections, and utility restoration efforts in different areas of the city.[59]

The Ushahidi maps for Haiti and Christchurch also included information gathered from the social media sites Facebook and Twitter.[60] On-line volunteers around the world turned social media reports into posts located on the Ushahidi map. A process to filter information, eliminate duplicate items and verify facts was used to lend validity to the information.[61]

Social media is newly recognized as a source of intelligence for responding authorities. FEMA Administrator Craig Fugate, in an address to a Senate Sub-committee, said,

> "…individuals, families and communities are our nation's 'first' first responders. The sooner we are able to ascertain the on-the-ground reality of a situation, the better we will be able to coordinate our response effort in support of our citizens and first responders. Through the use of social media, we can disseminate important information to individuals and communities, while also receiving essential real-time updates from those with first-hand awareness."[62]

Twitter is especially valuable as it allows a user to search for and follow information, not just individuals. While any single user's eyewitness account of an incident or event may not be credible, the technique of "crowdsourcing"[63] allows analysis of multiple reports of the same event, increasing the credibility of the information.

The United States Southern Command (SOUTHCOM) uses social media to "provide greater situational awareness to facili[ta]te faster responses."[64] Employing a Twitter search dashboard called TweetGrid,[65] their Operations Center learned of the Haiti earthquake while the ground was still shaking, well before news organizations reported it.

Social media also can allow emergency managers and their public information officers easy avenues to communicate pertinent information to the public without having to wait for the traditional print or broadcast media news cycle. Immediately after the Christchurch earthquake, for example, Twitter was used to direct people to areas of shelter, fresh water and clothing distribution points, and to relay information about the restoration of utilities.

By canvassing partner agencies and the public to determine the most appropriate and necessary information, and by quickly making that information available directly to the people affected by the disaster; the task of caring for the victims can become easier.

NIMS calls for the establishment of a Joint Information Center (JIC) and for public information to "be coordinated and integrated across jurisdictions and across jurisdictions, agencies, and organizations; among Federal, State, tribal, and local governments; and with NGOs and the private sector."[66] In many cases, the public affairs capabilities the military brings to a disaster will greatly assist the JIC mission.

Disaster response information can take many forms. Although programs and platforms will continue to change, and innovations will continue to advance, planners must remain flexible in their approaches and keep in mind that coordination is key to their ability to partner with other agencies.[67]

<u>When</u> *and* ***<u>Where</u>***. When and where will the information be needed? Most information exchanges occur via the Internet; beginning in some cases even before a domestic emergency event occurs. RECOMMENDATION: Regular and routine access to systems and password protected accounts must be maintained as part of steady state operations to ensure availability whenever required.

Access to information related to emergencies may be required from the highest levels of government to responders on-site and to the public. Many important decisions related to resourcing and supplying disaster areas are made in operations centers that are located a great distance from the incident site or affected area, though. Decision makers at a distance are relying only on information gained from those present at the incident site as a basis for their judgments.

It is important for the most credible, clear, concise, and correct information to be made available to these parties so they may maintain situational awareness and make timely, quality decisions. It is also important that easily attainable, appropriate information be available to the pre-staged or on-site response partners who may face challenges due to disaster related service interruptions, overloads in internet and cellular phone services, or have equipment with limited connectivity.

Although the use of cellular services ultimately proved resilient in Haiti, many cell towers were destroyed when the buildings that supported the towers collapsed. In other cases, system components were shaken out of alignment and required attention from technicians before they could be put back into operation.[68] Because of the limited availability of the system, and the lower quality of service requirements for data as compared to voice traffic, the SMS text messaging employed was very successful for communications in the affected area.[69]

Data takes on many different forms for many different users, but it is undisputed that appropriate data reach the response partners. It also holds true that timely data is required throughout the entire cycle of an event.

<u>How</u>. How will the information be coordinated, transmitted, received and used, and how will the integrity and security of the information be maintained? RECCOMENDATION: The military and other agencies likely to respond to disasters must build relationships at all levels to ensure they are ready to work together when called.

At the federal level, the 2010 Quadrennial Defense Review calls for the improvements in DSCA support and states, “the Department of Defense will closely cooperate with other U.S. departments and agencies to better protect and advance America’s interests.”[70] To this end, DOD and DHS are in the process of implementing a Strategic Operations Information Sharing Plan,[71] and Secretary of Defense has convened a Defense Science Board Task Force on Achieving Interoperability in a Net-Centric Environment. Their product dives deeply into technical issues focused mainly on DOD interoperability, but also considered DHS interoperability during domestic emergency response.[72] While this level of interagency cooperation calls for formal agreements, governance, testing, and accreditation; smaller scale information sharing relationships must also be considered.

It is essential that state, tribal, county and local level entities strengthen their abilities to work together, and with private and public entities at their levels. The National Fire Protection Association (NFPA), an internationally recognized code making body recognized as an authority for reduction of the burden of fire and other hazards, created Code 1600, the *Standard on Disaster/Emergency Management and Business Continuity Programs*. It advocates coordination and advisory committees as well as training and exercises to prepare for the implementation of disaster plans.[73] Similarly, recommendations resulting from the 2010 Haiti earthquake include “engag[ing] in preparation and simulation exercises…for future emergency responses…to identify models for how formal institutions and self-organized efforts on the ground interact during humanitarian response.”[74]

One important aspect associated with information sharing for the myriad of disaster response partners is establishing mechanisms to trust other users in order to ensure information integrity. In this context, a trusted entity is one that provides some assurance that the sender or receiver of information is actually who they claim to be, based on their user name or account name. Untrusted entities may not necessarily be who they claim to be when there is no mechanism provided for verification.

DOD user trust is based on a non-repudiation mechanism provided by a unique and private key held by each user's common access card and a personal identification number that is required to use the card. This assures senders, for example, that email actually came from the named user's account. Other users with government or corporate domains may have assurances built into their processes that make it likely that a user is actually who they claim to be. Public email services, however, such as G-mail or Hotmail,[75] offer no such means to validate user names.

Information flow can certainly be maintained to and from untrusted users, but trusted users may benefit from access to additional information, such as CUI or otherwise sensitive information that is restricted to others. Guidance for information classifications, handling and access should be another point of coordination among partners.

During their response to the Haiti earthquake, SOUTHCOM established a Community of Interest (COI) on the All Partners Access Network (APAN). APAN is a file sharing portal created to provide "effective information exchange and collaboration between [DOD] and any external country, organization, agency or individual that does not have ready access to traditional DOD systems and networks."[76] Another such endeavor by the DOD's Joint Knowledge Online (JKO), is HARMONIEWeb. It provides an environment to "forge trusted working relationships between government and non-government organizations in a trusted environment....while keeping out those whose interests are not so noble."[77] Both sites employ techniques to validate users or domains in order to limit access to untrusted entities.

DHS has established similar capabilities in the Homeland Security Information Network (HSIN). It "is a national secure and trusted web-based portal for information sharing and collaboration between federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission."[78]

Each site offers a slightly different collection of tools for communicating and sharing information related to disaster management. Some individual states have also undertaken efforts to provide information sharing platforms for partner agencies.[79] RECOMMENDATION: Arrangements to ensure the most likely partners or domains are appropriately credentialed should be included in early coordination efforts.

Other coordination points for local and regional partners include email communications and file sharing portal access, regular directory maintenance, understandings of file types and sizes to be exchanged, and estimations of bandwidth capacities that users expect to have available. They may also include password protected access to Incident Management Systems, and guidelines for monitoring or using the information contained on those systems. RECOMMENDATION: These points should be written into EMAC agreements or memorandums of understanding between partner agencies.

Similar points also accompany layer sharing for common operating pictures. DOD's APAN, the National Guard's Geospatial Information Center (GIC),[80] and a DHS product called Virtual USA[81] provide common interface points for such layer exchange. Other, similar endeavors include NORTHCOM's Situational Awareness Geospatial Enterprise (SAGE)[82] and DHS's Integrated Common Analytical Viewer (iCAV) and DHS

Earth, providing access to many critical infrastructure and homeland security related data layers.[83]

Responders close to disaster areas may count on cell phone networks as their primary mode of voice and data communications. Even though networks make efforts to harden their systems and provide redundancy, network availability may not be a realistic expectation immediately after the disaster. In some cases, cellular companies may bring in portable cellular assets to supplement or replace damaged parts of their system,[84] leaving those voice and data services degraded in the hours immediately after the incident. Coordination with these service providers may aid in infrastructure restoration that is critical to responders.

Responding agencies and their counterparts should understand how communications degradation may affect them in the first hours after a disaster. Coordination with other partners to share satellite access may be very valuable. Because of the possibility of limited availability of cell networks, SMS text messaging in lieu of voice operations also proves viable. SMS allows for data to be automatically resent if the first transmission is unsuccessful. Cellular systems also have the capability, if configured appropriately, to accommodate bulk message broadcasts in a manner that minimizes the impact to the cellular network.[85] Knowing which agencies and numbers are equipped to receive SMS text messages is certainly a valuable planning point as well.

Incorporating social media before disaster strikes involves establishing accounts and gaining and maintaining a following of partner agencies and users by establishing a presence on the services and providing useful information on a regular basis. This could include reposting or retweeting useful information from partner agencies and ensuring that local news media follow and repost pertinent information.[86] During a disaster, early monitoring of social media messages and establishment of simple keywords (called hashtags)[87] is vital to gain new followers and increase the span of coverage. Twitter even offers a feature for users to monitor trends in hashtags so popular topics can easily be identified.

Trusted user status is very difficult on social media such as Twitter. The site has had a process in place to verify or trust users claiming to be celebrities. It may be possible, in the future, for public officials and disaster response agencies to petition for similar status. In the meantime, Twitter recommends users link to a twitter identity from an official website.[88]

Putting trust in individual social media users is even more difficult for emergency managers and partner agencies, and manually evaluating this data can be very time consuming. The creators of Ushahidi have developed a free, open-source product called Swiftriver to sort and filter data and impart a degree of trust and verification into crowdsource data. It was “born out of the need to understand and act upon a wave of massive amounts of crisis data that tends to overwhelm in the first 24 hours of a disaster.”[89] “The software…is based on the idea that by comparing messages and information from a variety of sources about an event, the system can build an understanding of which are credible and which are not.”[90]

RECOMMENDATION: Any of the tools described should be explored before disaster strikes to build operator proficiencies before they are required. The operational tempo after an event is sometimes too high to allow for the associated learning curve.

Summary

Early establishment of partner relationships and periodic contact to maintain coordination is vital to successful working relationships and information sharing mechanisms. Domestic operations partners, including military elements, must be cognizant of the fact that it is impossible to imagine every partner agency to be involved before the disaster strikes. Planning and training on new partner coordination may make these actions easier after disaster has struck.

The need for information sharing among domestic operations partners is apparent, and the requirements seem to be growing almost as fast as solutions are developed or adapted. It is essential for planners to focus on interoperability and flexibility, steering away from proprietary systems and other limiting factors that may preclude adaption as technology changes. This will better facilitate interoperability with other response partners.

Certainly, pre-established relationships and mechanisms for information sharing must be established prior to disasters in order to save valuable time in the crucial hours immediately after disaster strikes. DOD must proactively engage their most likely response partners to build relationships and begin coordination efforts. These relationships should be periodically revisited, and key points of coordination periodically reviewed and maintained to ensure that the DOD homeland defense and disaster relief responders are prepared and equipped to aid in a fully coordinated response by exchanging appropriate information in a timely manner with DOD partner organizations.

Endnote

[1] Charles Rogriguez, Bernd McConnel and Kristine Shelstad, "Support to Disaster Response: The Science and Art of Disaster Response by the National Guard," *Center for Army Lessons Learned Newsletter* 10-16 (February 2006): 39; available from: https://call2.army.mil/toc.aspx?document=116#, Internet.

[2] *Civil Support Operations,* Headquarters, Department of the Army, FM 3-28 (Draft: 29 June 2010): 1-13; available from: http://usacac.army.mil/cac2/FM3-28/FM328.pdf, Internet.

[3] President, "Homeland Security Presidential Directive 5: Management of Domestic Incidents," *U.S. Department of Homeland Security*, (February 2003); available from: http://www.dhs.gov/xabout/laws/gc_1214592333605.shtm, Internet.

[4] "Introducing National Response Framework," *U.S. Department of Homeland Security*, (January 2008): 3; available from: http://www.fema.gov/emergency/nrf/aboutNRF.htm, Internet.

[5] Tribal government entities are commonly listed in emergency management documents including the National Response Framework. FEMA refers to the Title 25 (Indians) and Title 43, Chapter 33 (Alaska Native Claims Settlement) in defining Indian Tribes and Tribal Governments in "Disaster Assistance Policy 9521.4: Administering American Indian and Alaska Native Tribal Government Funding," *Federal Emergency Management Association*, (April 2007); available from: http://www.fema.gov/government/grant/pa/9521_4.shtm, Internet.

[6] Introducing NRF, 3.

[7] The term mutual aid/assistance agreement as used here includes cooperative agreements, partnership agreements, memoranda of understanding, intergovernmental compacts, or other terms commonly used for the sharing of resources. "Standard on Disaster/Emergency Management and Business Continuity Programs," *National Fire Protection Association*, (2007 ed.) NFPA 1600, [CD-ROM], (National Fire Codes Subscription Service, Electronic Edition, Fall 2008), Appendix A.

[8] Title 32 of the US Code outlines the dual status role of members of the National Guard, serving under the Governor of each state or territory until order to active duty (Title 10) status, serving under the command of the President of the United States. The Governor has the ability to mobilize Soldiers and Airmen to state active duty status according to the laws of their State. In this status, the provisions of the Posse Comitatus Act do not apply. "National Guard Fact Sheet Army National Guard (FY2005)," *Army National* Guard; available from: http://www.arng.army.mil/SiteCollectionDocuments/Publications/News%20Media%20Factsheets/ARNG_Factsheet_May_06%20ARNG%20fact%20Sheet.pdf, Internet.

[9] The Federal share for assistance provided under this title (section) shall not be less then 75 percent of the eligible costs (of such assistance). "Title 44 CFR 206.65," *GPO Access: Electronic Code of Federal Regulations*; available from: http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=cb026ad7b49625e3d72368148b7e0bfb&rgn=div8&view=text&node=44:1.0.1.4.57.3.18.5&idno=44, Internet, and "Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, and Related Authorities," *Federal Emergency Management Agency,* (June 2007) FEMA 592, 28; available from: http://www.fema.gov/pdf/about/stafford_act.pdf, Internet, also known as Public Law 93-288, as amended, 42 U.S.C. 5121-5207.

[10] Terry Scherling, "Examining the Military's Support of Civil Authorities during Disasters," (prepared statement to House of Representatives, Committee on Homeland Security, Subcommittee on Emergency Communications, Preparedness, and Response, 110th Cong., 1st sess., Washington, D.C., 25 April, 2007): 6; available from: http://www.fas.org/irp/congress/2007_hr/disaster.pdf, Internet.

[11] Emergency Management Assistance Compact agreements are created between states to provide civilian and military assistance. P.L. 104-321, administered by National Emergency Management Association. Procedures allow reimbursement for personnel and equipment and define liability issues. "About EMAC: What is EMAC?" *National Emergency Management Association*; available from: http://www.emacweb.org/?9, Internet.

[12] *Stafford Act*, 28.

[13] "National Response Framework," *U.S. Department of Homeland Security*, (January 2008): 6; available from: http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf, Internet.

[14] Title 10 of the US Code defines the role of the active duty military and the reserve component of the armed forces. The provisions of the Posse Comitatus Act typically apply to the duties of Title 10 Soldiers serving in the Continental United States. "Title 10 – Armed Forces," *Cornell University Law School*; available from: http://www.law.cornell.edu/uscode/uscode10/usc_sup_01_10.html, Internet.

[15] *Department of Defense Dictionary of Military and Associated Terms*, Department of Defense, JP 1-02, (8 November 2010, as amended through 31 January 2011): 100; available from: http://www.dtic.mil/doctrine/dod_dictionary, Internet. Also found in *Civil Support,* Department of Defense, JP 3-28 (14 September 2007): GL-7; available from: http://www.dtic.mil/doctrine/new_pubs/jp3_28.pdf, Internet.

[16] According to Assistant Secretary of Defense for Homeland Defense Paul McHale. "McHale: Disaster Response Time Expected to Improve." *National Defense* 90, no. 630 (2006): 10; available from: http://www.thefreelibrary.com/McHale%3a+disaster+response+time+expected+to+improve.-a0145836347, Internet.

[17] Sgt. Sara Wood, "DOD Leaders Report on Hurricane Response," *American Forces Information Service News Articles* (10 November 2005); available from: http://osd.dtic.mil/news/Nov2005/20051110_3310.html, Internet.

[18] "Any occurrence, resulting from the use of chemical, biological, radiological and nuclear weapons and devices; the emergence of secondary hazards arising from counterforce targeting; or the release of toxic industrial materials into the environment, involving the emergence of chemical, biological, radiological and nuclear hazards." JP 1-02, 51. A CBRN event may be a manmade attack: such as an intentional sarin gas or radiological explosive (dirty bomb) attack, or intentionally spread biological event (anthrax or botulism contamination); manmade accident such as a chemical or nuclear plant incident; or natural occurrence, such as a pandemic influenza epidemic.

[19] JP 1-02, 114. Also found in *Homeland Security,* Department of Defense, JP 3-27 (12 July 2007): GL-8; available from: http://www.dtic.mil/doctrine/new_pubs/jp3_27.pdf, Internet.

[20] Rodriguez, 41.

[21] GEN James Cartwright, (speech presented to the general session of the National Guard Bureau's 2011 Domestic Operations Workshop, National Harbor, Maryland, 20 January 2011).

[22] Ibid.

[23] The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, (February 2006), by Frances Fragos Townsend, 50; available from: http://georgewbush-whitehouse.archives.gov/reports/katrina-lessons-learned/, Internet.

[24] Controlled unclassified information (CUI) is defined by Executive Order 13556, dated November 4, 2010. "Presidential Documents: Executive Order 13556," *Federal Register* 75, no. 216, (November 9, 2010); available from http://frwebgate.access.gpo.gov/cgi-bin/getpage.cgi?position=all&page=68675&dbname=2010_register, Internet. Controlled unclassified information (CUI) is defined for the purposes of military compliance with this executive order by: *Operations Security*, Department of the Army, AR-530-1, (19 April 2007): 25; available from: http://armypubs.army.mil/epubs/530_series_collection_1.html, Internet.

[25] Sensitive information is defined by: *The Computer Security Act of 1987*, Public Law 100-135 (8 January 1988); available from: http://www.nist.gov/cfo/legislation/Public%20Law%20100-235.pdf, Internet.

[26] Protected Critical Infrastructure Information is defined in *Critical Infrastructure Information Act of 2002*, Public Law 107-296 (25 November 2003); available from: http://www.dhs.gov/xlibrary/assets/CII_Act.pdf, Internet.

[27] Health insurance information security is defined in *Health Insurance Portability and Accountability Act of 1996*, Public Law 104-191. "Summary of the Privacy Rule," OCR Privacy Brief, Office of Civil Rights, Department of Health and Human Services (May 2003); available from: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html, Internet.

[28] *Freedom of Information Act (FOIA)*, Public Law 104-231; available from: http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm, Internet. For Official Use Only designations on documents produced by the U.S. Military are governed by: *The DOD Freedom of Information Act Program*, Department of Defense Regulation 5400.7-R (September 1998); available from: http://www.dtic.mil/whs/directives/corres/pdf/540007r.pdf, Internet.

[29] These steps are also in keeping with the Federal Emergency Management Agency's National Emergency Communications Plan recommendations. "Frequently Asked Questions," Communications and Information Management, Federal Emergency Management Agency; available from: http://www.fema.gov/emergency/nims/CommunicationsInfoMngmnt.shtm, Internet.

[30] Commonly referred to as the '.mil' or 'dot mil' domain.

[31] Gina Pace, "Mexico Sends First-Ever Aid North: 'Act of Solidarity' Brings Supplies, Specialists to the U.S.," *CBS News* (7 September 2005); available from: http://www.cbsnews.com/stories/2005/09/07/katrina/main824295.shtml, Internet.

[32] Christopher Evanson, “Canadian Beacon-Operation Unison,” *Coast Guard Magazine*, Katrina The Gulf Response, Special Edition 2005, reprint, *Mariners Weather Log*, National Oceanic and Atmoshperic Administration, 50, no. 1 (April 2006); available from: http://www.vos.noaa.gov/MWL/apr_06/canada.shtml, Internet.

[33] “Strategic Operations Information Sharing Plan of Action,” *Canada Command Joint Command Centre and NORAD and USNORTHCOM Command Center*, (18 December 2009); available from: https://www.intelink.gov/inteldocs/action.php?kt_path_info=ktcore.actions.document.view&fDocumentId=236155, Internet.

[34] “Corporate Factsheet: Walmart by the Numbers,” Walmart (March 2010); available from: http://walmartstores.com/download/2230.pdf, Internet.

[35] Bryan Koon, “Emergency Management in the Private Sector,” (speech presented to the general session of the 2010 New Madrid Seismic Zone Workshop, Camp Robinson, North Little Rock, Arkansas, September 15, 2010).

[36] Ibid.

[37] E. Noam and H. Sato, “Kobe’s lesson: dial 711 for ‘open’ emergency communications,” *Science*, 274, no. 5288 (1 November 1996): 739-740; available from: http://www.citi.columbia.edu/elinoam/articles/kobe.htm, quoted in Anthony Townsend and Mitchell Moss, “Telecommunications Infrastructure in Disasters: Preparing Cities for Crisis Communications,” Center for Catastrophe Preparedness and Response & Robert F. Wagner Graduate School of Public Service, New York University (April 2005): 38; available from: http://www.nyu.edu/ccpr/pubs/NYU-DisasterCommunications1-Final.pdf, Internet.

[38] Belgrade, formerly capitol of Yugoslavia, is now the capitol of the country of Serbia.

[39] EL Quarantelli, “The Disaster Research Center (DRC) Field Studies of Organized Behavior in the Crisis Time Period of Disasters,” Disaster Research Center, University of Deleware (1997), quoted in Townsend, *Telecommunications Infrastructure in Disasters*, 34.

[40]“From Disaster to Community Development: The Kobe Experience,” United Nations Center for Regional Development (January 17, 2003); available from: http://www.hyogo.uncrd.or.jp/publications/documents/kizuna.pdf, quoted in Townsend, *Telecommunications Infrastructure in Disasters*, 34.

[41] Townsend, *Telecommunications Infrastructure in Disasters*, 34.

[42] Anne Nelson and Ivan Sigal with Dean Zambrano, *Media, Information Systems and Communities: Lessons from Haiti* (Report for the John S. and James L. Knight Foundation): 12; available from: http://issuu.com/knightfoundation/docs/kf_report_haiti_english_01.10.11?mode=embed&layout=http%3A%2F%2Fskin.issuu.com%2Fv%2Flight%2Flayout.xml&showFlipBtn=true, Internet, and “Home,” Christchurch Recovery Map; available from: http://eq.org.nz/main, Internet.

[43] Geotagging, also referred to as geo-referenced information or geospatial information “…is marking a video, photo or other media with a location.” Daniel Nations, “What is

Geotagging?" *About.com: Web Trends*; available from: http://webtrends.about.com/od/glossary/a/what-geotagging.htm, Internet.

[44] Microsoft® and SharePoint® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

[45] ESi® and WebEOC® are registered trademarks of ESi Acquisition, Inc. Product data sheet listing WebEOC clients; available from: http://esi911.com/esi/index.php?option=com_content&task=view&id=33&Itemid=44, Internet.

[46] NC4™ and E Team are registered trademarks of NC4. Product data sheet available from: http://www.nc4.us/eteam.php, Internet.

[47] "Homeland Defense, Homeland Security and Civil Support Strategic Operations Information Sharing: Operating Concept and Implementation Framework," *Department of Defense*, (Draft, 15 March 2010); available from: https://www.intelink.gov/inteldocs/action.php?kt_path_info=ktcore.actions.document.view&fDocumentId=237255, Internet.

[48] Communications and Information Management.

[49] ArcGIS® is a trademark or registered trademark of Environmental Systems Research Institute, Inc. (ESRI) in the United States, the European Community, or certain other jurisdictions.

[50] Google Earth™ is a trademark or registered trademark of Google®.

[51] Common file formats include KML, KMZ and GeoRSS. KML, formerly known as Keyhole Markup Language when it was originally developed, is now an open standard officially named the OpenGIS® KML Encoding Standard (OGC KML) maintained by the Open Geospatial Consortium, Inc. (OGC), "KML Reference," Google Code; available from: http://code.google.com/apis/kml/documentation/kmlreference.html, Internet. KMZ files are compressed collections of KML files, "KMZ Files," Google Code; available from: http://code.google.com/apis/kml/documentation/kmzarchives.html, Internet. GeoRSS (Geographical information sent with RSS – Really Simple Syndication, a common web feed format) with GML, Geographical Markup Language, is another format for modeling, transport, and storage of geographic information, "Geographical Markup Language (GML) WG," Open Geospatial Consortium, Inc.; available from: http://www.opengeospatial.org/projects/groups/gmlwg, Internet.

[52] Nelson, 5.

[53] Nelson, 4.

[54] Short codes are special telephone numbers, shorter than regular numbers, designed to facilitate easy SMS text services. Nelson, 12.

[55] Nelson, 15.

[56] Nelson, 13.

[57] Ushahidi is "open source software for information collection, visualization and interactive mapping….using multiple channels, including SMS, email, Twitter and the web." "Ushahidi Home Page," Ushahidi; available from http://www.ushahidi.com, Internet.

[58] The bandwidth restrictions experienced by the Marines in this case could apply to any organization, military or otherwise, depending on their organic equipment and what they have available. This example highlights how it is helpful for data to be made available across different platforms. Ibid.

[59] "Home," Christchurch Recovery Map; available from: http://eq.org.nz/main, Internet.

[60] Nelson, 15, and "Becoming a Volunteer," Christchurch Recovery Map; available from: http://eq.org.nz/page/index/9, Internet.

[61] "Becoming a Volunteer."

[62] Craig Fugate, "Understanding the Power of Social Media as a Communication Tool in the Aftermath of Disasters," (testimony before the Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Disaster Recovery and Intergovernmental Affairs, Washington, D.C., 05 May 2011); available from: http://www.dhs.gov/ynews/testimony/testimony_1304533264361.shtm, Internet.

[63] "Crowdsourcing, a term coined by Jeff Howe in a June 2006 issue of *Wired* magazine, is a model of labor that has been fully embraced on the Internet….[and] takes tasks traditionally done by a single person or small groups of people, and farms them out to a global workforce. The large-scale committee approach is powerful because it leans on the concept of the "wisdom of crowds" (to a certain extent) which says basically that the more input, the better the output." Jeff Howe, "The Rise of Crowdsourcing," *Wired* 14, no. 06 (June 2006); available from: http://www.wired.com/wired/archive/14.06/crowds.html, Internet, quoted in Josh Cantone, "Your Guide to the Crowdsourced Workforce," *The ReadWriteWeb* (12 May 2008); available from: http://www.readwriteweb.com/archives/crowdsourced_workforce_guide.php, Internet, and Kim Stephens, "Crisis Mapping, Crisis Crowdsourcing and Southern Storms," *idisaster 2.0: Social Media and Emergency Management* (8 May 2011); available from: http://idisaster.wordpress.com/2011/05/08/crisis-mapping-crisis-crowdsouring-and-southern-storms/, Internet.

[64] Corey McKenna, "Social Network Adds Situational Awareness to Haitian Earthquake Response," *Emergency Management* (June 30, 2010); available from: http://www.emergencymgmt.com/safety/Social-Network-Situational-Awareness-Haiti-Earthquake.html, Internet.

[65] "TweetGrid is a powerful Twitter Search Dashboard that allows you to search for up to 9 different topics, events, conversations, hashtags, phrases, people, groups, etc in real-time. As new tweets are created, they are automatically updated in the grid. No need to refresh the page!" "FAQ," Tweetgrid; available from http://tweetgrid.com/faq, Internet. TweetDeck (http://www.tweetdeck.com) is another Twitter dashboard that is currently popular.

[66] National Incident Management System," *U.S. Department of Homeland Security* (December 2008): 70; available from: http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf, Internet.

[67] Greg Hapgood, Iowa National Guard Public Affairs Officer (with Joint Information Center experience during domestic operations), interview by author, written notes, Johnston, IA, 02 May 2011.

[68] Anne-Marie Corley, "Why Haiti's Cellphone Networks Failed: Haitian engineer Charles-Edouard Denis describes the cellular landscape before and after Haiti's quake," *IEEE Spectrum* (February 2010); available from: http://spectrum.ieee.org/telecom/wireless/why-haitis-cellphone-networks-failed/2, Internet.

[69] Xiaoqiao Meng et. al., *Analysis of the Reliability of a Nationwide Short Message Service*, (Paper prepared for IEEE, INFOCOM 2007, 26th IEEE International Conference on Computer Communications, 6-12 May 2007) 1811-1819; available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.76.2465&rep=rep1&type=pdf, Internet.

[70] As an example, in Title 10 status, NORTHCOM is funded for some interagency coordination, like the National Level Exercise (NLE) program conducted with DHS. National Guard State HQs fund interagency coordination through their Domestic Operations staffs. Specific unit activities must be funded from operational accounts as training or reimbursed for actual responses. "Quadrennial Defense Review," *Department of Defense* (February 2010): xiv; available from: http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf, Internet.

[71] "Homeland Defense, Homeland Security and Civil Support Strategic Operations Information Sharing".

[72] "Creating an Assured Joint DOD and Interagency Interoperable Net-Centric Enterprise," *Defense Science Board Task Force on Achieving Interoperability in a Net-Centric Environment*, *Office of the Under Secretary of Defense for Acquisition, Technology and Logistics*, (March 2009); available from: http://www.acq.osd.mil/dsb/reports/ADA498577.pdf, Internet.

[73] NFPA 1600, Appendix A.

[74] Nelson, 24.

[75] Gmail™ is a Google® service and Hotmail® is a Microsoft® service. Both provide free web-based email accounts to users.

[76] All Partner Access Network was formerly known as the Asia-Pacific Area Network. "About Us," *All Partner Access Network*; available from: https://community.apan.org/p/about.aspx, Internet.

[77] "Partner Organizations," *HarmonieWEB*; available from: http://www.harmonieweb.org/PartnerOrganizations/Pages/default.aspx, Internet.

[78] "Homeland Security Information Network," *Department of Homeland Security*; available from: http://www.dhs.gov/files/programs/gc_1156888108137.shtm, Internet.

[79] Alabama, Florida, Louisiana, Oregon and Virginia have State Information-Sharing Capabilities. "Virtual USA," FirstResponder.gov, Department of Homeland Security; available from: http://www.firstresponder.gov/Pages/VirtualUSA.aspx, Internet.

[80] “National Guard Common Operational Picture,” *Intellipedia*; available from: https://www.intelink.gov/wiki/National_Guard_Common_Operational_Picture, Internet.

[81] Virtual USA “focus[es] on cross-jurisdictional information sharing and collaboration among the homeland security and emergency management community.” Virtual USA.

[82] “Situational Awareness Geospatial Enterprise,” *United States Northern Command*; available from: https://sageearth.northcom.mil, Internet.

[83] “Integrated Common Analytical Viewer (iCAV),” *Department of Homeland Security*; available from: http://www.dhs.gov/files/programs/gc_1217445858859.shtm, Internet.

[84] “Network Facts: Network Reliability,” Verizon Wireless (April 2011); available from: http://aboutus.vzw.com/bestnetwork/network_facts.html, Internet.

[85] Meng.

[86] According to COL Greg Hapgood, Public Affairs Officer for the Iowa National Guard, equality among news organizations is very important. Care must be taken to ensure all organizations are offered the same opportunities to utilize social media content. Hapgood interview.

[87] “Hashtags are a community-driven convention for adding additional context and metadata to Twitter messages (tweets). They are contained in the body of the message and are created by prefixing a key word with a hash symbol: #hashtag. Hashtags were developed as a means to create ‘groupings’ on Twitter, without having to change the basic service. Using the correct key word is important so the message can be accessed by the appropriate followers.” “CampCrisisNZ FAQ,” *Crisis Commons*; available from: http://wiki.crisiscommons.org/wiki/CrisisCampNZ_volunteer_FAQ, Internet. Additional information available from “What are Hashtags? (“#” Symbols), *Twitter Help Center*; available from: http://support.twitter.com/entries/49309-what-are-hashtags-symbols; Internet.

[88] “About Verified Accounts,” *Twitter Help Center*; available from: http://support.twitter.com/groups/31-twitter-basics/topics/111-features/articles/119135-about-verified-accounts, Internet.

[89] “Home,” *Swiftriver*; available from: http://swift.ushahidi.com/, Internet.

[90] Matthew Ingram, “Swift River: Trying to Filter the Social Web Firehose,” *Gigaom* (26 July 2010); available from: http://gigaom.com/2010/07/26/swift-river-trying-to-filter-the-social-web-firehose/, Internet.